COMMITTEE ON HOMELAND SECURITY

The "Raising the Bar Act"

Introduced by Chairman Max Rose (D-NY)
of the Intelligence and Counterterrorism Subcommittee

The proliferation of terrorist content online is not a new phenomenon. Despite social media companies' efforts to block such content on their sites, terrorist content – like that of the March 15th attacks against the Muslim Community in Christchurch, New Zealand– can still be found online. Studies have shown that mass killings can inspire copycats,[1] raising concerns that terrorist content that goes viral on social media platforms may inspire other acts of mass violence. Additionally, ideologically-motivated mass killings may inspire retaliatory attacks. Immediately following the Christchurch attack, FBI and DHS advised law enforcement officials to "remain vigilant in light of the enduring threat to faith-based communities posed by domestic extremists (DEs), as well as by homegrown violent extremists (HVEs) who may seek retaliation."[2] Tragically, in the months since the Christchurch attack, several domestic terrorists made reference to this Christchurch attacker's manifesto and drawn inspiration from those attacks.

The magnitude of this homeland security challenge demands partnership between the social media companies, groups engaged in civil society efforts, and the Federal government at an unprecedented level. Social media companies cannot effectively address it alone. The **Raising the Bar Act** seeks to encourage collaborative efforts between social media companies, civil society groups and the Federal government to address online terrorist content in a manner that champions transparency, civil rights, civil liberties, and privacy. Inspired by the *European Union's Code of Conduct on countering illegal hate speech online* that has helped social media companies remove illegal speech from their sites, this bill would:

- **Direct the Department of Homeland Security (DHS) to designate a lead institution to administer a voluntary online terrorist content moderation exercise program.** The lead institution would design and administer a voluntary online terrorist content moderation exercise program to test how well participating technology companies adhere to their own content moderation policies and procedures. In the process of designing and administering the voluntary exercise program, the lead institution, in collaboration with the participating technology companies, would identify **trusted flaggers** to participate in the program, such as civil society partners involved in identifying domestic and international terrorism trends, academics, nonprofits, technology companies.

---

[1] *See, e.g.,* Maggie Fox, *Mass killings inspire copycats, study finds*, NBC NEWS, July 2, 2015, https://www.nbcnews.com/health/health-news/yes-mass-killings-inspire-copycats-study-finds-n386141; *Number of mass shootings in US has risen sharply, FBI report says,* THE GUARDIAN, Sep. 25, 2014, https://www.theguardian.com/world/2014/sep/25/us-mass-shootings-risen-sharply-fbi-report ("'The copycat phenomenon is real,' said Andre Simons of the FBI's Behavioral Analysis Unit. 'As more and more notable and tragic events occur, we think we're seeing more compromised, marginalized individuals who are seeking inspiration from those past attacks.'")

[2] *Joint Intelligence Bulletin: Attacks on Mosques in Christchurch, New Zealand, May Inspire Supporters of Violent Ideologies*, DEPT. OF HOMELAND SECURITY, FEDERAL BUREAU OF INVESTIGATION, NATIONAL COUNTERTERRORISM CENTER, Mar. 15, 2019, https://publicintelligence.net/dhs-fbi-nctc-christchurch-attacks/.

- **Require the lead institution to produce a report after each exercise program that will grade the technology companies on their efforts.** The contents of the report will track how technology companies perform and rate them based on objective criteria. Specifically, the companies would be judged based on their:
    - responses to notifications from trusted flaggers;
    - transparency efforts and redress methods; and
    - investment in solutions to study and counter terrorist content online.

- **Establish a public-private partnership.** The bill directs DHS to enter into public-private partnership with participating technology companies in which the companies agree to cover at least 80 percent of the costs of the exercise program. The bill authorizes $300,000 for the first year, and $150,000 annually thereafter to DHS to carry out the program. The bill allows for the lead institution, on a case-by-case basis, to provide payments to trusted flaggers to participate in exercises.

- **Require a Report by the Government Accountability Office (GAO).** Requires the GAO to review the implementation of the exercise program and submit the report to Congress within 180 days after receiving the sixth exercise report.

- **Require a congressional briefing.** After each monitoring exercise, the House Committee on Homeland Security and the Senate Committee on Homeland Security and Governmental Affairs would be briefed on the results of the voluntary online terrorist content moderation exercise program.